

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

United States of America,

Criminal No. 15-20 PJS/JJK

Plaintiff,

v.

REPORT AND RECOMMENDATION

Frank Russell McCoy,

Defendant.

Katharine T. Buzicky, Esq., Assistant United States Attorney, and Jeffrey
H. Zeeman, Esq., Dept. of Justice, for the Plaintiff, United States of
America;
Michael C. Hager, Esq., for Defendant Frank Russell McCoy.

JEFFREY J. KEYES, United States Magistrate Judge

INTRODUCTION

The Court held hearings in this matter on June 29, 2015, and July 29, 2015. The Court issued an Order on Motions dated June 29, 2015, addressing certain discovery and disclosure related issues. The Court reserved issuing proposed findings of fact and conclusions of law on Defendant's motions to suppress statements and to suppress evidence obtained as a result of search and seizure. The Court heard testimony and received exhibits at the June 29, 2015 hearing with regard to suppression of seized evidence and statements. Subsequently, the Court reopened the motions hearing and received additional testimony during a second hearing on July 29, 2015.

Based on the file and documents contained therein, along with witness testimony and exhibits presented at the hearings, and the memoranda of counsel, this Court recommends that Defendant's suppression motions be denied for the reasons that follow.

I. BACKGROUND

A. Seizure and Search

Defendant was indicted in the Middle District of Georgia in June 2007 on a count of transportation of obscene matter. The indictment was based on emails sent by the Defendant that included obscene stories, which contained descriptions of murder, rape, and sexual assault of children. He was arrested in Minnesota on January 9, 2008, pursuant to a Georgia warrant. Later that month he was arraigned in the Middle District of Georgia and was released on a \$25,000 unsecured bond. The conditions of release included the condition that he not own, possess, or use a computer without the permission of a pre-trial services officer.

On June 3, 2009, U.S. Magistrate Judge Richard L. Hodge modified the conditions of Defendant's release to allow Defendant to use a computer and the Internet to conduct legal research and communicate with counsel, access government websites, access specified reference material websites, and play games. On June 24, 2010, a second Order Modifying Conditions of Release was issued by U.S. Magistrate Judge Thomas Q. Langstaff providing that:

(1) The defendant can use and access the internet and email for all lawful purposes; (2) the defendant's use and access of email and the Internet shall be permitted, provided that he does not transmit any of the stories that are subject of the instant case, or stories and materials of a similar nature; (3) and, provided that he will be subject to random inspections of his computer's internet and email usage history by the Pre-trial Services Officer assigned to his case, in order to ensure compliance with the parameters of these conditions. However his correspondence with his attorney shall not be subject of such inspections.

In 2013, following a bench trial before U.S. District Court Judge W. Louis Sands, the Defendant was convicted on the obscene materials charge in the Georgia case. In August 2013, Defendant was sentenced to 18 months imprisonment and two years supervised release. He was initially placed in Bureau of Prisons custody, but on September 24, 2013, the Court granted bond and released Defendant while his case was on appeal on the same conditions that had been stated in the June 24, 2010 pre-trial release order.¹ Defendant was allowed to stay at his Minnesota residence.

Defendant's prosecution and supervised release remained venued in the Middle District of Georgia, but U.S. Probation Officer Timothy Norgren was assigned courtesy supervision over the Defendant in Minnesota. On December

¹ The September 24, 2013 order included a complete restriction on the defendant's use of the Internet, but on October 2, 2013, the Court issued a clarifying Order explaining that the order granting bond pending appeal was amended to "to allow Defendant use of the internet in accordance with the conditions previously set by United States Magistrate Judge Thomas Q. Langstaff in his January 24, 2010 Order, including the inspection requirements set forth in same." (Hrg. Ex. 1.)

18, 2013, Officer Norgren asked that U.S. Probation Officer Lisa Martinetto accompany him on a routine check of the Defendant's residence pursuant to the conditions of release imposed by the Georgia court. Officer Norgren requested Officer Martinetto's assistance because of her expertise with computers.

Officers Norgren and Martinetto knocked at Defendant's residence door, and he answered and invited the officers to enter. Officer Martinetto had not previously met the Defendant. Defendant was cordial towards the officers as they walked through Defendant's split level home. In plain view, Officer Martinetto observed several computers, in various stages of construction or assembly, scattered throughout the house. The Defendant talked to Martinetto about building his own computers and programming them in 50 different computer languages. There were at least two custom-built computers in the residence and multiple computers that Defendant was in the process of repairing. One of the custom-built computers had five hard drives in it, including three working together in a RAID system. According to Officer Martinetto, it is very unusual for a personal computer user to have a computer with multiple hard drives and to have such a sophisticated RAID system, which is typically used in connection with computer servers.

Defendant told Martinetto that he had written a program to eliminate the pornography on his computers, so he was ready for her to look at them and asked her to look at his computers. Officer Martinetto declined Defendant's offer to check computer hardware contents when she was at Defendant's home on

December 18, 2013. She knew that the home visit was being conducted pursuant to supervised release conditions under the Georgia bond order, but she was not fully aware of the extent of supervisory authority granted in the Georgia case, and she concluded that it would not have been feasible to examine the equipment in the home at that time due to the large volume of electronic storage equipment at the residence. At some point Officer Norgren advised Officer Martinetto that he had only been aware of one laptop computer being used by the Defendant and that he was surprised by the number of computers now in the house.

In light of the observations at Defendant's home, Officer Martinetto contacted Anthony Lindsey, Defendant's assigned Probation Officer in Georgia, for guidance and clarification on permissible computer usage. Officer Lindsey advised Officer Martinetto that pursuant to the June 24, 2010 Order, Defendant was allowed to use a computer for limited purposes only, and his computers were subject to random examination. Officer Lindsey then consulted the presiding judge in the Georgia case, Hon. W. Louis Sands, regarding the circumstances. After consulting with the Deputy Chief of Probation, Officer Lindsey proposed that they acquire the computer media discovered by Officer Martinetto and examine it. According to Officer Lindsey, Judge Sands wanted to make sure that Defendant was obeying the conditions of release and was not disseminating obscene material or possessing, disseminating, or receiving child pornography. Judge Sands directed Officer Martinetto to remove the computers

that she already knew to be located in the residence or which the defendant volunteered were in his possession for further examination. (Doc. No. 56, Tr. of June 29, 2015 Hr'g ("6/29/15 Tr.") 19–20.)

Officer Martinetto and two other probation officers went to Defendant's residence on January 10, 2014. The officers entered and walked through the house with no objection from the Defendant. They removed a self-built tower that contained five hard drives, a second self-built tower located in a lower-level bedroom with two hard drives, and a computer on the dining room table that also contained two hard drives. Officer Martinetto had observed all of this equipment on her previous visit to Defendant's residence. The three officers also removed a laptop that Defendant claimed he had forgotten to tell Officer Martinetto about during her previous visit. The Defendant also provided Officer Martinetto with six USB drives that were located in plain view on his desk. (*Id.*) Officer Martinetto explained to Defendant that, per her agreement with the Northern District of Georgia Probation Office, she would be sending all of those hard drives to Georgia for further review.

The seized computer hard drives and thumb drives were sent by FedEx to the Department of Probation in Georgia for inspection of the contents. The items were received by U.S. Probation Officer Todd Garrett, a specialist in computer media search and inspection, which Officer Garrett performed on the

seized computer hard drives.² In the process of conducting his forensic analysis, Officer Garrett followed the standard practice of first creating a bit-for-bit forensic copy of each of the original drives. Officer Garrett produced the copies to allow search and inspection of those drives while preserving the integrity of the original drives. Officer Garrett used various technological tools and software, including a Tableau write blocker, which prevents alterations to the original drives during copying, a Forensic Toolkit, and encase Forensic Software. All of these are industry-accepted computer investigation tools.

When Officer Garret finished imaging the drives, he noted that one of the drives was in an unformatted state, meaning that the normal directories, subdirectories, and the folders or files that one might expect in a Windows installation were not present. Officer Garrett testified that such data storage configuration is sometimes the result of a user attempting to prevent data from being seen, and a layperson looking at a computer in an unformatted state would not be able to gain information about Internet use. Officer Garrett then did a file header search on the unformatted drive, looking specifically for .JPEG image files which often indicate a user's web-browsing activities. The file header search revealed the existence of images of prepubescent children on the drive, including images depicting children engaged in sexually explicit conduct. Officer Garrett

² Officer Garrett has a Certified Forensic Computer Examiner designation from the International Association of Computer Investigative Services and has obtained a computer forensics specialist designation from Guidant Software.

found that the .JPEG images of child pornography were derived from video files, which are often obtained via the Internet.

USPO Garrett explained, as a general matter, that forensic examiners are unable to ascertain the full scope of Internet activity based solely on examining web browser activity. (Doc. No. 59, Tr. of July 29, 2015 Hr'g ("7/29/15 Tr.") 35.) Furthermore "[t]here is no one central repository for Internet artifacts on a computer hard drive and the Windows operating system." (*Id.*) USPO Garrett further noted that, in his opinion, it would have not been "forensically appropriate" to have turned on Defendant's computer in his residence to examine his web browser for Internet activity. (*Id.* at 37.) That type of analysis would not "preserve the state and integrity of the original media" in the state it was originally found. (*Id.*)

As a result of Officer Garrett's discovery, on March 14, 2014, U.S. Magistrate Judge Thomas Q. Langstaff issued a warrant authorizing the complete search of all of the computer media removed from Defendant's home. The warrant identified each of the devices to be searched, and described the objects to be seized as evidence of violation of United States statutes prohibiting the transportation, distribution, receipt, accessing, and possession of visual depictions of minors engaged in sexually explicit conduct. Magistrate Judge Langstaff issued the warrant on the basis of asserted in the Affidavit of United States Department of Homeland Security Special Agent Cory E. Brant. The warrant application states the statutory basis for the suspected offense, the

evidentiary and legal basis for seizure of the hard drives, and probable cause in support of the warrant request, consisting of the in-home observations of Officer Martinetto and the preliminary analysis of the computer hard drive contents by probation officers in Georgia.

Defendant's supervised release in Georgia was revoked following the execution of the search warrant which resulted in the discovery of more images of child pornography; he was required to serve his term of imprisonment on the transportation of obscene matters conviction. The indictment in this case charging Defendant with possession of child pornography is based on the images obtained as a result of the execution of the same search warrant.

B. Statements

When the probation officers were in Defendant's home on December 18, 2013 and January 10, 2014, Defendant engaged in conversation with the officers about his computer use and expertise. This included a statement by Defendant that he had performed a wiping program on his electronic storage devices to remove pornography, so he was ready for Officer Martinetto to look at the computers. Defendant seeks to suppress any statements that he made to the probation officers during these two visits to his home.

II. ANALYSIS

A. Search and Seizure

Defendant contends that the government violated his Fourth Amendment rights when the computer media was seized in Minnesota and examined by

Officer Garrett in Georgia, and he moves to suppress the evidence of child pornography obtained in that examination.

At the time of the computer drive seizures and searches in this case, the effective court order regarding the Defendant's supervised release stated:

(1) The defendant can use and access the internet and email for all lawful purposes; (2) the defendant's use and access of email and the Internet shall be permitted, provided that he does not transmit any of the stories that are subject of the instant case, or stories and materials of a similar nature; (3) and, provided that he will be subject to random inspections of his computer's internet and email usage history by the Pre-trial Services Officer assigned to his case, in order to ensure compliance with the parameters of these conditions. However his correspondence with his attorney shall not be subject of such inspections. (Hrg. Ex. 1).

The terms of supervised release thus authorized the probation officers to conduct random inspections of Defendant's Internet and email usage to ensure that he was not engaged in unlawful activity which, in his case, would obviously be focused on activity related to child pornography. While the Defendant concedes that the Probation Officers could randomly inspect his computers to insure that he was complying with the conditions of release, he contends that the Probation Officers should have searched his computers where he preferred (his home), and under the conditions that he preferred (on-site triage). However, there were no such limitations in the supervised release order. On-site review and inspection of the Defendant's computers was not necessary, and indeed it was not feasible in this case. There were a large volume of hard drives present,

and the Probation Officers were justifiably concerned about the Defendant's ability to hide or erase child pornography.

The Defendant told Officer Martinetto that he had programmed computers in many different computer languages and he had built two of the computers in his house. One of the computers was a tower with five hard drives - one running Windows, one running DOS, and three in a RAID system, which is commonly used when a computer is utilized as a server, not for typical personal use. The Probation Officers were obviously dealing with a person with a very high degree of sophistication in computer use. Indeed, the Defendant admitted to having used a program to wipe his computers of pornography, so there was a reasonable expectation that something much more than a cursory on-site review of online historical activity would be required.

Moreover, as Officer Garrett, a computer expert, explained, forensics examiners are unable to ascertain the full scope of Internet activity based solely on examining web browser activity and on-site examination of the web browser for Internet activity would not preserve the integrity of the original media in the state it was originally found.

Officer Garrett's preliminary inspection of the computer hard drives that were seized was well within the scope of the supervised release order. He first used forensics software to create a mirror image copy of the nine hard drives. When he completed the imaging, Officer Garrett noticed that one of the drives appeared to be in an unformatted state. He focused his attention on this

unformatted drive because, based on his training and experience, he knew that a user might reformat a drive to prevent data that once existed on the drive from being seen. Within one hour of commencing his search, Garrett observed that the unformatted hard drive contained images depicting pre-pubescent children engaged in sexually explicit conduct. He then determined that these still images were derived from full child pornography videos stored on the seized hard drives. Officer Garrett knew that evidence of this nature is often obtained through the Internet, both via web browsers and through other means. This evidence was used as a basis to obtain the search warrant to conduct the complete search of the hard drives.

Defendant argues that Officer Garrett's inspection "went well beyond the conditions of release to inspect not only Internet or email, but extensive user files. Under the conditions of release, this was an unreasonable search." (Doc. No. 60, Def.'s Second Post-Hearing Mem. ("Def.'s Second Mem.") 10.) However, the supervised release order did not require that the inspection be conducted in any specific manner. And there was no requirement that the probation officers had to have any level of suspicion of unlawful activity before the random inspection occurred. "Random" inspection is just that: an inspection that can occur at any time without any prior investigation of wrongdoing that would justify it. Given all of these circumstances, the warrantless seizure and examination of Defendant's computers did not violate Defendant's Fourth Amendment right to be free of unreasonable search and seizure. See *Samson v.*

California, 547 U.S. 843 (2006) (upholding warrantless, suspicionless searches of individuals on supervision); *United States v. Smith*, 655 F.3d 839, 846 (8th Cir. 2011) (district court may impose suspicionless search conditions), *rev'd on other grounds by Smith v. United States*, 132 S. Ct. 2712 (2012).³

B. Search Warrant

In support of his motion to suppress evidence obtained during the search of his computer hardware pursuant to the March 14, 2014 warrant (Hrg. Ex. 2), Defendant argues only that the warrant was invalid because it was based on the allegedly illegal seizure of his hard drives on January 10, 2014 and its subsequent unlawful examination by Officer Garrett. (See Def.'s Second Mem. 11.) However, as explained above, there was nothing unlawful about the seizure of Defendants hard drives, nor about Officer Garrett's preliminary examination. Thus, the evidence obtained pursuant to the search warrant was not the fruit of an unlawful seizure and search of the computer drives.

³ The Government argues, in the alternative, that Defendant gave his consent to the warrantless seizure of his computers and their subsequent inspection by Officer Garrett. The Government bases this argument on comments made by the Defendant during the first visit that Officer Martinetto could look at his computer and Defendant's cooperative demeanor during the second visit when the computers were seized. The Court does not construe Defendant's statement and demeanor, or his lack of vocal objection to the officers, as amounting to sufficient evidence of consent. However, in light of the fact that, as explained above, the seizure of the computers and their inspection were authorized by the conditions of release, Defendant's consent was not required for the search and seizure to pass constitutional scrutiny.

Moreover, as determined United States Magistrate Judge Thomas Q. Langstaff, this Court concludes that the search warrant was based on sufficient probable cause as stated in the Affidavit of United States Department of Homeland Security Special Agent Cory E. Brant. The warrant also properly and sufficiently identified the devices to be searched and the objects of the warrant.⁴

C. Statements

Defendant was not under arrest nor in custody when he made statements to probation officers during a routine supervised release check on December 18, 2013, and a supervised release visit on January 10, 2014 to seize computer drives. The officers did not subject Defendant to direct questioning or its functional equivalent. They did not compel Defendant to be present or accompany them as they conducted the supervised release check. Defendant made his statements freely and voluntarily. The officers made no promises or threats, nor did they coerce Defendant to make the statements.

Defendant argues that his statements must be suppressed because he was not provided with the warnings required by *Miranda v. Arizona*, 384 U.S. 436, 444, 86 S.Ct. 1602 (1966). (Def.'s Second Mem. 10–11.) However,

⁴ In any event, this Court concludes that the good faith exception under *United States v. Leon*, 468 U.S. 897 (1984), applies with respect to execution of the search warrant in this case. “[A]bsent allegations that the [issuing judge] was not neutral, ‘suppression is appropriate only if the officers were dishonest or reckless in preparing the affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause.’” *United States v. Formaro*, 152 F.3d 768, 771 n.4 (8th Cir. 1998) (quoting *Leon*, 468 U.S. at 926).

Miranda warnings are only required prior to custodial interrogation, and Defendant was not in custody at the time he made the statements to probation officers in his home.

In considering whether the Defendant was in custody during questioning the court must assess the totality of the circumstances. *United States v. Axsom*, 289 F.3d 496, 500 (8th Cir. 2002). Custody occurs when the subject's freedom of action is limited in any significant manner. *Id.* at 500 (citing *United States v. Griffin*, 922 F.2d 1343, 1347 (8th Cir. 1990) and *Miranda v. Arizona*, 384 U.S. 436, 444, 86 S.Ct. 1602 (1966)). The court must consider the presence and extent of physical and psychological restraints upon the subject's liberty during questioning and thereafter determine whether a reasonable person in the suspect's situation would have understood that he was indeed in custody. *Id.* (citing *Griffin*, 922 F.2d at 1347). Indicia which are commonly applied in determining whether a suspect is in custody include:

(1) whether the suspect was informed that the questioning was voluntary and that the subject was free to leave or request that officers leave, or that the suspect was not under arrest; (2) whether the suspect possessed unrestrained freedom during questioning; (3) whether the suspect initiated contact with law enforcement or voluntarily acquiesced to requests for responses to questions; (4) whether strong arm tactics or deception were used during questioning; (5) whether the atmosphere of the questioning was police dominated; or (6) whether the subject was arrested at the conclusion of questioning.

Id., (citing *Griffin* at 1349).

Here, Defendant welcomed the probation officers into his house and voluntarily provided information in response to any questioning. Defendant's

freedom was unrestricted and he was free to leave at any time. The facts pertinent to the first three *Griffin* factors strongly suggest that Defendant was not in custody when he provided the statements at his own residence. The probation officers also used no strong arm tactics. The atmosphere of the questioning was not police dominated, and the officers never threatened Defendant with arrest during either home visit. Nor was Defendant placed under arrest at the end of either encounter at his home. In essence, none of the aggravating factors weigh in favor of a conclusion that the Defendant was in custody at any time on either December 18, 2013 or January 10, 2014.

Under the circumstances of the interviews at issue, there was no requirement that the Defendant be advised of his rights per *Miranda*, the meetings did not take place in a coercive setting, and Defendant was not arrested and was free to leave at any time. Defendant's statements to probation officers should not be suppressed.

RECOMMENDATION

The Court hereby recommends that:

1. Defendant Frank Russell McCoy's Motion to Suppress Evidence be **DENIED** (Doc. No. 28); and

2. Defendant Frank Russell McCoy's Motion to Suppress Statements, Admissions and Answers Made by Defendant to Law Enforcement Officers that the Government Intends to Use at Trial be **DENIED** (Doc. No. 29).

Dated: October 1, 2015

s/ Jeffrey J. Keyes
JEFFREY J. KEYES
United States Magistrate Judge

Under Local Rule 72.2(b) any party may object to this Report and Recommendation by filing with the Clerk of Court, and serving all parties by October 14, 2015, a writing which specifically identifies those portions of this Report to which objections are made and the basis of those objections. Failure to comply with this procedure may operate as a forfeiture of the objecting party's right to seek review in the Court of Appeals. A party may respond to the objecting party's brief within fourteen days after service thereof. All briefs filed under this rule shall be limited to 3500 words. A judge shall make a de novo determination of those portions of the Report to which objection is made. This Report and Recommendation does not constitute an order or judgment of the District Court, and it is therefore not appealable directly to the Circuit Court of Appeals.

Unless the parties stipulate that the District Court is not required by 28 U.S.C. § 636 to review a transcript of the hearing in order to resolve all objections made to this Report and Recommendation, the party making the objections shall timely order and file a complete transcript of the hearing within ten days of receipt of the Report.